

דיברנו על פונקציות אגרגציה הן פונקציות שמחזירות ערך אחד, למשל: count, sum, max, min, avg

אם למשל נירצה למצוא איזה ספר זמין בכמות הגדולה ביותר בטבלה Available :

נסיון ראשון:

```
SELECT ISBN, MAX(noOfCopies)
FROM Available
```

מה קורה? למה זה לא עובד? אנחנו מנסים לשלב כאן פונקציה אגרגציה עם בחירת שורות פשוטה. זה לא ילך. על מנת לעשות זאת יש שתי אפשרויות. אפשרות אחת להשתמש ב-sub query ואפשרות שניה

להשתמש במה שניקרא: **GROUP BY**

האפשרות הראשונה:

```
SELECT ISBN
FROM Available
WHERE noOfCopies = (
  SELECT MAX(noOfCopies)
  FROM Available
)
```

הנה האפשרות השנייה:

```
SELECT ISBN, MAX(noOfCopies)
FROM Available GROUP BY ISBN
```

ניתן גם להוסיף WHERE clause לפקודת ה-SELECT למשל: WHERE ISBN > 5555555555, אבל המיקום של ה-WHERE יהיה לפני ה-GROUP BY מה שעושה ה-Where, זה להגביל את בחירת השורות הכללית מהטבלה, ועל שורות אלה תופעל ההקבצה של שורות על פי השדה (או שדות) של ה-Group by

למשל:

```
SELECT column_name, aggregate_function(column_name)
FROM table_name
WHERE column_name operator value
GROUP BY column_name
```

### שימוש ב-GROUP BY ו-HAVING

השימוש הראשון שנראה זה מציאת ספרים שמופיעים למשל במלאי של יותר מספריה אחת. לשם כך נבצע אגרגציה של מספרי ISBN ונציין count(\*) כדי לדעת בכמה ספריות הם נימצאים (לא משנה מספר העותקים). לשם כך נכתוב:

```
SELECT ISBN, COUNT(*)
FROM Available
GROUP BY ISBN
HAVING COUNT(*) > 1;
```

פקודת ה-Having עבור ה-Group by היא מעין "Where" - כלומר מגבילה את הקבוצות שיופיעו בטבלת התוצאה.

שימוש נוסף שנראה יהיה לשם מציאת ספרים (מס זיהוי) שעבורם כמות העותקים שנתורה בכל הספריות בהן הם נימצאים, גדול-2. כלומר כאן פונקציה האגרגציה לא סתם תספור שורות אלא תסכם גם את כמות העותקים בכל השורות בהן הספר מופיע.

ובכן, מצא את כל הספרים שיש מהם יותר משני עותקים זמינים בסך הכל בכל הספריות האפשריות. בתוצאה הצג כל ספר והכמות שנותרה ממנו זמינה בסך הכל.

```
SELECT ISBN, SUM(noOfCopies)
FROM Available
GROUP BY ISBN
HAVING SUM(noOfCopies) > 2
```

## המשך הדיון על הצפנה

אם לא ניתן להסיק מ- $e$  את  $d$ , אפשר ש- $e$  יהיה מידע ציבורי כך שכל אחד יוכל להצפין את הודעתו, ורק זה שיש לו את קוד הפיענוח -  $d$  יוכל לקרוא את ההודעה. **שיטה זו ניקראת: public/private**

בחלק ב של הרצאה זו, נתאר אלגוריתם בשם RSA שמיועד ליצור שיטה של: **public/private**

ישנה שיטת הצפנה סימטרית שאפשר לאמר שהיא בטוחה לחלוטין (מבחינה הסתברותית), אולם אינה שימושית במיוחד.

דמיינו שמפתח הצופן הוא קוד בינארי שמוצר בצורה רנדומלית והוא באורך ההודעה (מתורגמת לבינארי) ושיטת ההצפנה היא יצירת  $exclusive\ or$  בין הביטים של ההודעה ושל הצופן ( $xor$ ). כאשר הצד המפענח מפעיל שוב את ה- $xor$ , הוא יקבל את ההודעה המקורית.

לדוגמה, ההודעה היא: 001101101 והצופן הוא: 010101010 במצב כזה לאחר הצפנה נקבל: 011000111 וכדי לפענח נבצע שוב  $xor$  עם 010101010 ונקבל: 001101101 (שהיא ההודעה המקורית).

לאחר שימוש בהודעה אחת נזרוק את הצופן, כי אם נשתמש בו בהודעות אחרות, אפשר יהיה לנחש דברים אם מאזין מרושע הצליח לקבל את ההודעות המוצפנות ( $c$ ) באנגלית בוב ואליס הם הטובים, איב ומאלורי הרעים (איב זה מ- $eves\ dropping$ , ומאלורי זה מהמילה:  $Malicious$ ), קארול נאיבית ( $care\ free$ )

כל אתר אינטרנט שמבטיח מידע שמגיע אליו משתמש בשיטה של  $public/private$ . **איך נידע שאנחנו מעבירים את כרטיס האשראי רק לאמזון?** נשתמש במפתח הצפנה ציבורי אבל הקוד לפיענוח נימצא אך ורק בידי אמזון וכמעט בלתי אפשרי למישהו אחר לנחשו, כך שאם מישהו האזין להודעה שלנו (המוצפנת) עדיין לא יוכל לנחש את מספר הכרטיס אשראי למשל.

איך אנחנו (המחשב שלנו) יודע שאנחנו מדברים עם אמזון ולא עם מתחזה?

אמזון רוצה להוכיח שהיא אמזון. היא אומרת לנו לבחור הודעה ונקרא לה:  $x$ . נישלח את  $x$  לאמזון. אמזון "תצפין" את  $x$  עם הקוד הפרטי שלה  $d$ , ותקבל את  $y$  שיהיה התוצאה של:  $D(d,x)$  אמזון תשלח אלינו חזרה את  $y$  (שהושג מ- $x$  ששלחנו על ידי הקוד הפרטי שיש רק לאמזון). כעת "נפענח" את  $y$  בעזרת הקוד הציבורי של אמזון  $e$  ונקבל את  $z$  על ידי:  $E(e,y)$ . אם  $z$  שווה ל  $x$ , הרי שאמזון הוכיחה לנו שהיא אכן אמזון. זאת כיוון ש:  $E(e,D(d,x))=x$  (ישנה סימטריה בהצפנה/פיענוח)

יכולה להיות כאן בעיה. מישהו בעבר, ניקרא לו בוב, עשה זאת עם אמזון ומישהו אחר (מרושע) שמו מאלורי הצליח להאזין ל  $x$  ול  $y$ . ואז מישהי בשם קרול רוצה לקנות ספר מאמזון ושולחת הודעה כדי לודא שהיא מדברת עם אמזון, במקרה הודעה זו היא כמו ה- $x$  ששלח בוב (נגיד Hello). מאלורי שמאזין על הקו, שולח לקרול את  $y$  שהוא כבר יודע ואז קרול חושבת שמאלורי זה אמזון ושולחת לו את כרטיס האשראי שלה. תמיד מניחים שאפשר להאזין ולקרוא את מה שעובר בשידור.